UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF COLORADO

MICHAEL KASSEM, and KIMBERLEY ROWTON, individually and on behalf of all others similarly situated, Plaintiffs, v. PINGORA LOAN SERVICING, LLC and PINGORA ASSET MANAGEMENT, LLC, Defendants.	Case No. **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

Plaintiffs Michael Kassem ("Kassem"), and Kimberley Rowton ("Rowton") (collectively, "Plaintiffs"), individually and on behalf of all other similarly situated individuals (the "Class Members," as defined below), by and through their counsel, file this Class Action Complaint against Pingora Loan Servicing, LLC and Pingora Asset Management, LLC (collectively, "Pingora" or "Defendant") and allege the following based on personal knowledge of facts pertaining to themselves and on information and belief based on the investigation of counsel as to all other matters.

I. NATURE OF THE ACTION

1. Pingora is a loan servicing provider that performs servicing duties, such as payment collection, to mortgage lenders. In this role, Pingora collects and stores the personal identifiable information ("PII") of thousands of individuals whose mortgages are, or were, serviced by Pingora.

2. This class action seeks to redress Pingora's unlawful, willful and wanton failure to reasonably protect the sensitive PII of Plaintiffs and Class Members (as defined below), in

violation of Defendant's legal obligations. Defendant failed to properly safeguard and protect the PII in its possession, thereby allowing cybercriminals to steal Plaintiffs and Class Members' valuable PII from Pingora's inadequately secured computer network.

3. The data breach was discovered in December 2021, when Pingora learned that unauthorized users had gained access to Pingora's file servers.[1] Pingora investigated the attack with the assistance of third-party computer specialists. The investigation confirmed that certain files on Pingora's systems had been accessed without authorization between October 27, 2021 and December 7, 2021 (the "Data Breach" or "Breach").[2] The forensic investigation further determined that one or more of the potentially impacted files contained the sensitive PII of thousands of individuals.[3]

4. According to Pingora, the exposed PII included names, addresses, Social Security numbers, loan number, and other unspecified information provided in connection with loan applications, modifications, or servicing.[4]

5. Due to Defendant's negligence, cyber criminals obtained everything they need to commit identity theft and wreak havoc on the financial and personal lives of thousands of individuals.

6. Plaintiffs have already suffered harm as a result of the Data Breach. Following the Data Breach, Plaintiff Kassem has had a fraudulent unemployment claim filed in his name. Since the Data Breach, Plaintiff Rowton has had someone access one of her accounts and transfer money

[1] *See* Pingora's letter to Plaintiffs, attached hereto as Exhibits 1-2.

[2] *Id.*

[3] https://www.iowaattorneygeneral.gov/media/cms/462022_Pingora_Loan_Servicing_LLC_124F8E23630C2.pdff (last accessed May 2, 2022).

[4] *See* Exhibit 1.

from it. These experiences have and will cause these Plaintiffs significant actual damages and a significant amount of lost time and opportunity.

7. For the rest of their lives, Plaintiffs and the Class Members will have to deal with the danger of identity thieves possessing and misusing their PII. Even those Class Members who have yet to experience identity theft have to spend time responding to the Breach and are at an immediate and heightened risk of all manners of identity theft as a direct and proximate result of the Data Breach. Plaintiffs and Class Members have incurred and will continue to incur damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of harm, damaged credit, deprivation of the value of their PII, loss of privacy, and/or additional damages as described below.

8. Plaintiffs bring this action individually and on behalf of the Class, seeking compensatory damages, punitive damages, restitution, and injunctive and declaratory relief, reasonable attorney fees and costs, and all other remedies this Court deems proper.

II. THE PARTIES

9. Plaintiff Kassem is domiciled in and a citizen of Georgia.

10. Plaintiff Kimberley Rowton is domiciled in and a citizen of Virginia.

11. Pingora Asset Management, LLC and Pingora Loan Servicing, LLC are Limited Liability Companies are registered in Wilmington, Delaware. Both maintain their principal place of business at 1819 Wazee Street, 2nd Floor, Denver, Colorado, 80202. Defendants can be served through their registered agent at: Corporation Service Company, 1900 W. Littleton Blvd., Littleton, Colorado 80120.

III. JURISDICTION AND VENUE

12. This Court has diversity jurisdiction over this action under the Class Action Fairness Act (CAFA),

13. 28 U.S.C. § 1332(d), because this is a class action involving more than 100 class members, the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and many members of the class are citizens of states different from Defendant.

14. This Court has personal jurisdiction over Defendant because its principal place of business is in this District, it regularly transacts business in this District, and many Class Members reside in this District. Venue is likewise proper as to Defendant in this District because Defendant employs a significant number of Class Members in this District, and a substantial part of the events or omissions giving rise to the claim occurred in this District. 28 U.S.C. § 1391(b)(2); *id.* at § 1391(f).

IV. FACTUAL ALLEGATIONS

A. The Data Breach

15. Based on information supplied by Pingora, the Data Breach was discovered in December 2021, when Pingora learned that unauthorized users had gained access to Pingora's file servers.[5] Pingora investigated the attack with the assistance of third-party computer specialists. The investigation confirmed that certain files on Pingora's systems had been accessed without authorization between October 27, 2021 and December 7, 2021.[6] The forensic investigation

[5] *See* Pingora's letter to Plaintiffs, attached hereto as Exhibits 1-2.

[6] *Id.*

further determined that one or more of the potentially impacted files contained the sensitive PII of thousands of individuals.[7]

16. According to Pingora, the exposed PII included names, addresses, Social Security numbers, loan number, and other unspecified information provided in connection with loan applications, modifications, or servicing.[8]

17. Pingora failed to take the necessary precautions required to safeguard and protect Plaintiffs' and the other Class Members' PII from unauthorized disclosure. Defendant's actions represent a flagrant disregard of the rights of its employees, applicants, business associates, and customers, both as to privacy and property.

18. Pingora further failed to provide Plaintiffs and Class Members with timely and accurate notice of the Data Breach. Instead, it took Pingora four months to warn Plaintiffs and Class Member of their imminent risk of identity theft. Defendant also failed to notify Plaintiffs and the Class Members precisely what personal information was compromised, leaving Plaintiffs and Class Members unsure as to the extent of the information that was exposed.

B. Plaintiffs' Experiences

Plaintiff Kassem

19. Upon information and belief, Pingora was responsible for servicing a mortgage loan that Plaintiff Kassem entered into in or around November 2019. As part of that mortgage loan, Plaintiff Kassem provided numerous categories of sensitive information likely including his name, address, telephone number, email address, date of birth, Social Security number, financial account

[7] https://www.iowaattorneygeneral.gov/media/cms/462022_Pingora_Loan_Servicing_LLC_124F8E23630C2.pdf.

[8] *See* Exhibit 1.

information, investment account information, information on other loans, employment information, and income information.[9]

20. In or around December 2021, Plaintiff Kassem was notified by the Georgia Department of Labor that someone had filed a fraudulent unemployment claim using his Social Security number.

21. In April 2022, Kassem received a breach notification letter from Pingora informing him that his personal information, including name, Social Security number, and other unspecified loan information had been exposed to cybercriminals during the Data Breach. The letter Kassem received is attached hereto as Exhibit 1.

22. Because the Data Breach was an intentional hack by cybercriminals seeking information of value that they could exploit, Plaintiff Kassem is at imminent and substantial risk of identity theft that is continuous and ongoing. Indeed, Plaintiff Kassem has already experienced identity fraud, as discussed above.

23. Plaintiff Kassem has spent numerous hours responding to the Data Breach and the identity theft that has occurred because of it. Among other things, Kassem has spent time monitoring his accounts and personal information, contacting the Georgia Department of Labor concerning the fraudulently filed unemployment claim, investigating the scope of the Data Breach, and taking other steps in an attempt to mitigate the adverse impact of the Data Breach. Due to the permanent and sensitive nature of some of the PII exposed in the Breach (such as Social Security numbers), Kassem will be required to continuously monitor his identity and credit for the rest of his life.

24. Kassem has been careful to protect and monitor his identity.

[9] *See* https://singlefamily.fanniemae.com/media/7896/display (Uniform Residential Loan Application).

25. To his knowledge, Kassem has not been the victim of any other data breach.

Plaintiff Rowton

26. Upon information and belief, Pingora was responsible for servicing a mortgage buyout that Plaintiff Rowton entered into in or around April 2021. As part of that mortgage loan, Plaintiff Rowton provided numerous categories of sensitive information likely including her name, address, telephone number, email address, date of birth, Social Security number, financial account information and statements, investment account information and statements, information and documentation of other loans, employment information such as W-2s, and income information such as tax reports.[10]

27. In or around January 2022, Plaintiff Rowton became aware that someone had used her PII to access one of her investment accounts and fraudulently transferred money from it.

28. In April 2022, Rowton received a breach notification letter from Pingora informing her that her personal information, including name, Social Security number, and other unspecified loan information had been exposed to cybercriminals during the Data Breach. The letter Rowton received is attached hereto as Exhibit 2.

29. Because the Data Breach was an intentional hack by cybercriminals seeking information of value that they could exploit, Plaintiff Rowton is at imminent and substantial risk of identity theft that is continuous and ongoing. Indeed, Plaintiff Rowton has already experienced identity fraud, as discussed above.

30. Plaintiff Rowton has had to spend significant time responding to the Data Breach, including time spent monitoring her accounts, contacting customer service for the fraudulently accessed investment account in an attempt to restore her funds, placing a freeze on all her credit

[10] *See* https://singlefamily.fanniemae.com/media/7896/display (Uniform Residential Loan Application).

reports, and otherwise attempting to mitigate the harms of the Breach. Due to the permanent and sensitive nature of some of the PII exposed in the Breach (such as Social Security numbers), Rowton will be required to continuously monitor her identity and credit for the rest of her life.

31. To Rowton's knowledge, she has not been the victim of any other data breach.

32. Plaintiff Rowton is very worried about the identity fraud she has already experienced and the significant risk of further identity fraud she now faces.

C. Cyber Criminals Have Used and Will Continue to Use Plaintiffs' PII to Defraud Them

33. PII is of great value to hackers and cyber criminals, and the data stolen in the Data Breach can and will be used in a variety of ways by criminals to exploit Plaintiffs and the Class Members and to profit off their misfortune.

34. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[11] For example, with the PII stolen in the Data Breach, including Social Security numbers, identity thieves can open financial accounts, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[12] These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and the Class Members.

[11] "Facts + Statistics: Identity Theft and Cybercrime," Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

[12] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

35. Social security numbers are particularly sensitive pieces of personal information. As the Consumer Federation of America explains:

> **Social Security number.** *This is the most dangerous type of personal information in the hands of identity thieves* because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refunds, employment – even using your identity in bankruptcy and other legal matters. It's hard to change your Social Security number and it's not a good idea because it is connected to your life in so many ways.[13]
>
> [Emphasis added.]

36. PII is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it for years.[14]

37. This was a financially motivated Breach, as the only reason the cyber criminals go through the trouble of running a targeted cyberattack against companies like Pingora is to get information that they can monetize by selling on the black market for use in the kinds of criminal activity described herein. Indeed, a social security number, date of birth, and full name can sell for $60 to $80 on the digital black market.[15] "[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web."[16]

38. These risks are both certainly impending and substantial. As the Federal Trade Commission ("FTC") has reported, if hackers get access to PII, they ***will*** use it.[17]

---

[13] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

[14] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/assets/270/262904.htmlu.

[15] Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web*, Nov. 15, 2017, https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web.

[16] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

[17] Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info.

39. Hackers may not use the information right away, but this does not mean it will not be used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information ***may continue for years***. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[18]

40. For instance, with a stolen social security number, which is part of the PII compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[19]

41. With this Data Breach, and as demonstrated by the identity theft Plaintiffs and other Class Members have already experienced, identity thieves have already started to prey on the Pingora breach victims, and we can anticipate that this will continue.

42. Identity theft victims like Plaintiffs as well as other Class Members, must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.[20]

43. Defendant's offer of one year of identity monitoring to Plaintiffs and the Class is woefully inadequate and will not fully protect Plaintiffs from the damages and harm caused by its failures. While some harm has begun already, as several Plaintiffs have already found out, the full scope of the harm has yet to be realized. There may be a time lag between when harm occurs

---

[18] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/assets/270/262904.htmlu.

[19] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

[20] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

versus when it is discovered, and also between when PII is stolen and when it is used. Once the twelve-months have expired, Plaintiffs and Class Members will need to pay for their own identity theft protection and credit monitoring for the rest of their lives due to Pingora's gross negligence. Furthermore, identity monitoring only alerts someone to the fact that they have *already been the victim of identity theft* (*i.e.*, fraudulent acquisition and use of another person's PII)—it does not prevent identity theft.[21] Nor can an identity monitoring service remove personal information from the dark web.[22] "The people who trade in stolen personal information [on the dark web] won't cooperate with an identity theft service or anyone else, so it's impossible to get the information removed, stop its sale, or prevent someone who buys it from using it."[23]

44. As a direct and proximate result of the Data Breach, Plaintiffs and the Class have suffered actual identity theft, have been damaged, and have been placed at an imminent, immediate, and continuing increased risk of harm from continued fraud and identity theft. Plaintiffs and the Class must now take the time and effort to mitigate the actual and potential impact of the Data Breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come. Even more seriously is the identity restoration that Plaintiffs and other Class Members must go through, which can include spending countless hours filing police reports, filling out IRS forms, Federal Trade Commission checklists, Department of Motor Vehicle driver's

[21] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, Nov. 30, 2017, https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html.

[22] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

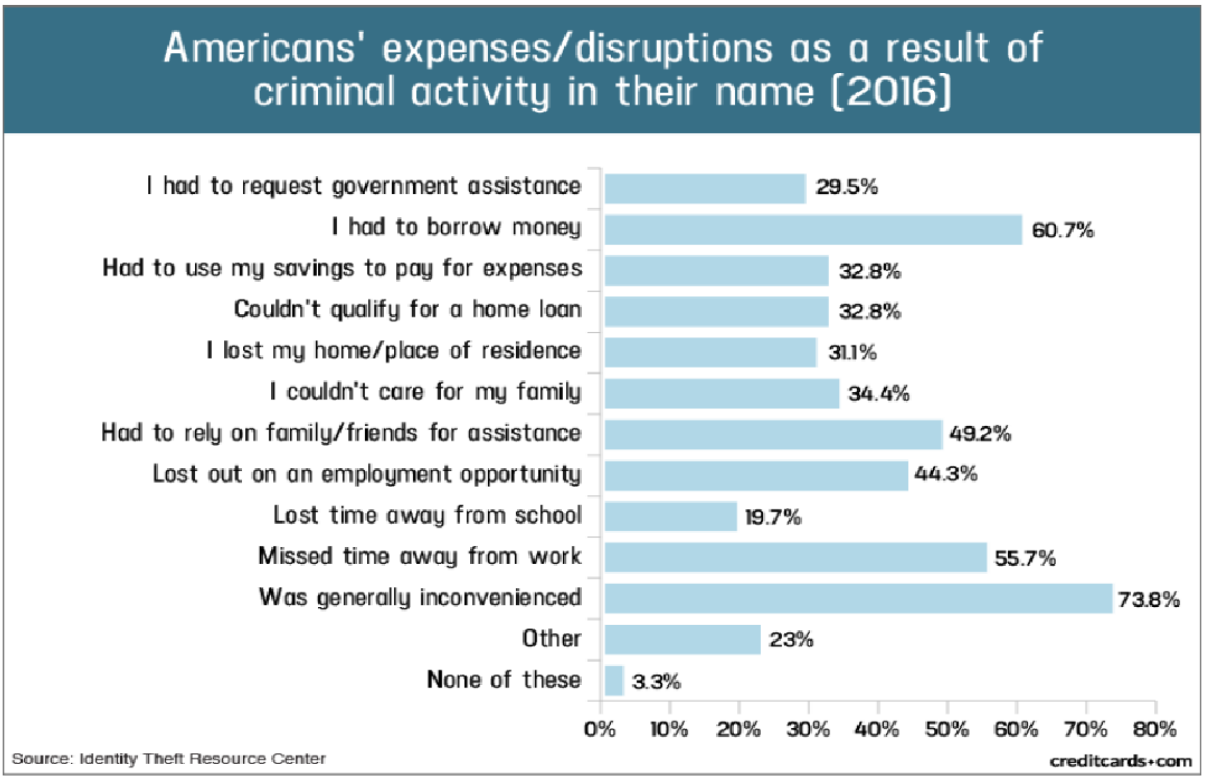
[23] *Id.*

license replacement applications, and calling financial institutions to cancel fraudulent credit applications, to name just a few of the steps Plaintiffs and the Class must take.

45. Plaintiffs and the Class have suffered, and continue to suffer, actual harms for which they are entitled to compensation, including:

a. Actual identity theft, including fraudulent credit inquiries and cards being opened in their names;
b. Trespass, damage to, and theft of their personal property including PII;
c. Improper disclosure of their PII;
d. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals and having been already misused;
e. Loss of privacy suffered as a result of the Data Breach, including the harm of knowing cyber criminals have their PII and that identity thieves have already used that information to defraud other victims of the Data Breach;
f. Ascertainable losses in the form of time taken to respond to identity theft and attempt to restore identity, including lost opportunities and lost wages from uncompensated time off from work;
g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach;
h. Ascertainable losses in the form of deprivation of the value of Plaintiffs' and Class members' personal information for which there is a well-established and quantifiable national and international market;
i. The loss of use of and access to their credit, accounts, and/or funds;
j. Damage to their credit due to fraudulent use of their PII; and
k. Increased cost of borrowing, insurance, deposits, and the inability to secure more favorable interest rates because of a reduced credit score.

46. Below is a chart that shows the kinds of expenses and disruptions that victims of identity theft experience[24]:



47. Moreover, Plaintiffs and Class Members have an interest in ensuring that their information, which remains in the possession of Defendant, is protected from further breaches by the implementation of industry standard security measures and safeguards. Defendant has shown itself wholly incapable of protecting Plaintiffs' PII.

48. Plaintiffs and Class Members also have an interest in ensuring that their personal information that was provided to Pingora years ago is removed from all Pingora servers, and especially from Pingora's unencrypted files.

[24] Jason Steele, *Credit Card and ID Theft Statistics*, CREDITCARDS.COM (Oct. 24, 2017), https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.

49. Defendant itself acknowledged the harm caused by the Data Breach because it offered Plaintiffs and Class Members the woefully inadequate twelve months of identity theft repair and monitoring services. Twelve months of identity theft and repair and monitoring is, however, inadequate to protect Plaintiffs and Class Members from a lifetime of identity theft risk.[25]

50. Defendant further acknowledged, in its letter to Plaintiffs and other Class Members, that Pingora needed to improve its security protocols, stating: "Pingora has implemented additional cybersecurity measures to further protect against similar incidents moving forward."[26]

51. The letter further acknowledged that the Data Breach would cause inconvenience to affected individuals and that financial harm would likely occur, stating: "We are notifying potentially impacted individuals, including you, so that you may take steps to protect your information. . . . We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors."

52. At Pingora's suggestion, Plaintiffs are desperately trying to mitigate the damage that Pingora has caused them. Given the kind of PII Pingora made accessible to hackers, however, Plaintiffs are certain to incur additional damages. Because identity thieves have their PII, Plaintiffs and all Class Members will need to have identity theft monitoring protection for the rest of their lives. Some may even need to go through the long and arduous process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with a new number.[27]

---

[25] *See* Exhibit 1, attached hereto.

[26] *Id.*

[27] *Will a New Social Security Number Affect Your Credit?*, LEXINGTON LAW (Nov. 16, 2015), https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html.

53. None of this should have happened.

D. Defendant was Aware of the Risk of Cyber Attacks

54. Data security breaches have dominated the headlines for the last two decades. And it doesn't take an IT industry expert to know it. The general public can tell you the names of some of the biggest cybersecurity breaches: Target,[28] Yahoo,[29] Marriott International,[30] Chipotle, Chili's, Arby's,[31] and others.[32]

55. Pingora as a service provider for mortgage loans, which requires collecting and maintaining highly sensitive and valuable PII, should certainly have been aware, and indeed was aware, that it was at risk for a data breach that could expose the PII that it collected and maintained.

56. With the increasing prevalence of data breach announcements, Pingora certainly recognized it had a duty to use reasonable measures to protect the wealth of PII that it collected and maintained.

57. Pingora was clearly aware of the risks it was taking and the harm that could result from inadequate data security.

---

[28] Michael Kassner, *Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned*, ZDNET (Feb. 2, 2015), https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/.

[29] Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*, CSOONLINE.COM (Oct. 4, 2017), https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html.

[30] Patrick Nohe, *The Marriot Data Breach: Full Autopsy*, THE SSL STORE: HASHEDOUT (Mar. 22, 2019), https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/.

[31] Alfred Ng, *FBI Nabs Alleged Hackers in Theft of 15M Credit Cards from Chipotle, Others*, CNET (Aug. 1, 2018), https://www.cnet.com/news/fbi-nabs-alleged-hackers-in-theft-of-15m-credit-cards-from-chipotle-others/?ftag=CMG-01-10aaa1b.

[32] *See, e.g.*, Taylor Armerding, *The 18 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Dec. 20, 2018), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

E. PINGORA COULD HAVE PREVENTED THE DATA BREACH

58. Data breaches are preventable.[33] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[34] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[35]

59. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[36]

60. In a Data Breach like this, many failures laid the groundwork for the Breach. The FTC has published guidelines that establish reasonable data security practices for businesses. The FTC guidelines emphasize the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[37] The guidelines establish that businesses should protect the confidential information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer

---

[33] Lucy L. Thomson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).

[34] *Id.* at 17.

[35] *Id.* at 28.

[36] *Id.*

[37] FTC, *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommended that businesses utilize an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating hacking attempts; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

61. Upon information and belief, Pingora failed to maintain many reasonable and necessary industry standards necessary to prevent a data breach, including the FTC's guidelines. Upon information and belief, Pingora also failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework, NIST Special Publications 800-53, 53A, or 800-171; the Federal Risk and Authorization Management Program (FEDRAMP); or the Center for Internet Security's Critical Security Controls (CIS CSC), which are well respected authorities in reasonable cybersecurity readiness.

62. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[38]

63. To prevent and detect malware attacks, including the malware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Federal Bureau of Investigation, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

[38] *See* How to Protect Your Networks from RANSOMWARE, at 3, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

- Configure firewalls to block access to known malicious IP addresses.

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[39]

[39] *Id.* at 3-4.

64. Further, to prevent and detect malware attacks, including the malware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[40]

[40] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://us-cert.cisa.gov/ncas/tips/ST19-001.

65. In addition, to prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

- **Secure internet-facing assets**
  - Apply latest security updates
  - Use threat and vulnerability management
  - Perform regular audit; remove privileged credentials
- **Thoroughly investigate and remediate alerts**
  - Prioritize and treat commodity malware infections as potential full compromise;
- **Include IT Pros in security discussions**
  - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;
- **Build credential hygiene**
  - Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords
- **Apply principle of least-privilege**
  - Monitor for adversarial activities
  - Hunt for brute force attempts
  - Monitor for cleanup of Event Logs
  - Analyze logon events
- **Harden infrastructure**
  - Use Windows Defender Firewall
  - Enable tamper protection
  - Enable cloud-delivered protection
  - Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[41]

[41] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/.

66. Given that Defendant was storing the PII of thousands of individuals, Defendant could and should have implemented all of the above measures to prevent and detect ransomware attacks.

67. Specifically, among other failures, Pingora had far too much confidential unencrypted information held on its systems. Such PII should have been segregated into an encrypted system.[42]

68. Moreover, it is well-established industry standard practice for a business to dispose of confidential PII once it is no longer needed. The FTC, among others, has repeatedly emphasized the importance of disposing unnecessary PII, saying simply: "Keep sensitive data in your system only as long as you have a business reason to have it. Once that business need is over, properly dispose of it. If it's not on your system, it can't be stolen by hackers."[43] Pingora, rather than following this basic standard of care, kept tens of thousands of former employees', applicants, business associates', and customers' unencrypted PII indefinitely. As a result, individuals who had stopped associating with Pingora several years earlier had their PII exposed in the Data Breach. This greatly expanded the number of victims harmed in the Breach.

69. In sum, this Data Breach could have readily been prevented through the use of industry standard network segmentation and encryption of all PII. Further, the scope of the Data Breach could have been dramatically reduced had Pingora utilized proper record retention and destruction practices.

F. Pingora's Response to the Data Breach is Inadequate to Protect Plaintiffs and the Class

[42] *See, e.g.*, Adnan Raja, *How to Safeguard Your Business Data with Encryption*, Aug. 14, 2018, https://digitalguardian.com/blog/how-safeguard-your-business-data-encryption.

[43] FTC, *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf at p. 6.

70. Pingora failed to inform Plaintiffs and Class Members of the Data Breach in time for them to protect themselves from identity theft.

71. Pingora stated that it discovered the Data Breach in August 2020. And yet, Pingora did not start notifying affected individuals until August 6, 2021—a full year after it learned of the Data Breach. Even then, Pingora failed to inform Plaintiffs and Class Members exactly what information was exposed in the Data Breach, leaving Plaintiffs and Class Members unsure as to the scope of information that was compromised.

72. During these intervals, the cybercriminals were exploiting the information while Pingora was secretly still investigating the Data Breach. For example, while Pingora was investigating the Breach, and had not notified impacted individuals, identity thieves had already begun stealing benefits by using the stolen names and Social Security numbers of breach victims, including Plaintiff Kassem who had an unemployment claim opened in his name shortly after the Data Breach.

73. If Pingora had investigated the Data Breach more diligently and reported it sooner, the damages could have been mitigated.

V. CHOICE OF LAW

74. Colorado has a significant interest in regulating the conduct of businesses operating within its borders. Colorado seeks to protect the rights and interests of citizens of the United States against a company headquartered and doing business in in its borders. Colorado has a greater interest in the nationwide claims of Plaintiffs and members of the Class (defined below) than any other state and is most intimately concerned with the claims and outcome of this litigation.

75. The corporate headquarters of Pingora, located in Denver, Colorado is the “nerve center” of its business activities – the place where its high-level officers direct, control, and

coordinate the company's activities, including its data security functions and major policy, financial, and legal decisions.

76. Defendant's response to the Data Breach at issue here, and the corporate decisions surrounding such response, were made from and in Colorado.

77. Defendant's breaches of duty to Plaintiffs and Class members emanated from Colorado

78. Application of the Colorado law to the Class with respect to Plaintiffs' and Class Members' claims is neither arbitrary nor fundamentally unfair because Defendant has significant contacts and a significant aggregation of contacts that create interest in the claims of Plaintiffs and the Class.

79. Under Colorado's choice of law principles, which are applicable to this action, the common law of Colorado applies to the nationwide common law claims of all Class Members.

VI. CLASS ACTION ALLEGATIONS

80. Plaintiffs incorporate by reference all preceding paragraphs as if fully restated here.

81. Plaintiffs bring this action against Pingora on behalf of themselves and all other individuals similarly situated under Federal Rule of Civil Procedure 23. Plaintiffs assert all claims on behalf of a nationwide class (the "Class") defined as follows:

> All persons whose personal identifiable information was compromised as a result of the Data Breach at Pingora between October 27, 2021 and December 7, 2021.

82. Excluded from the Class are Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and members of their immediate families and judicial staff.

83. Plaintiffs reserve the right to amend the above definition or to propose subclasses in subsequent pleadings and motions for class certification.

84. The proposed Class meets the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

85. **Numerosity:** The proposed Class is so numerous that joinder of all members is impracticable. Defendant has reported to the Iowa General's Office that the number of Iowans affected in the Data Breach was 9,817 individuals[44] and this does not include the affected individuals from other states.

86. **Typicality:** Plaintiffs' claims are typical of the claims of the Class. Plaintiffs and all members of the Class were injured through Pingora's uniform misconduct. The same event and conduct that gave rise to Plaintiffs' claims are identical to those that give rise to the claims of every other Class member because Plaintiffs and each member of the Class had their sensitive PII compromised in the same way by the same conduct of Pingora.

87. **Adequacy:** Plaintiffs are adequate representatives of the Class because Plaintiffs' interests do not conflict with the interests of the Class; Plaintiffs have retained counsel competent and highly experienced in data breach class action litigation; and Plaintiffs and Plaintiffs' counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and their counsel.

88. **Superiority:** A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiffs and the Class. The injury suffered by each individual class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for members of the

[44] https://www.iowaattorneygeneral.gov/media/cms/462022_Pingora_Loan_Servicing_LLC_124F8E23630C2.pdf.

Class individually to effectively redress Pingora's wrongdoing. Even if Class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

89. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiffs and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a. Whether Defendant engaged in the wrongful conduct alleged herein;

b. Whether Defendant failed to adequately safeguard Plaintiffs' and the Class's PII;

c. Whether Defendant owed a duty to Plaintiffs and the Class to adequately protect their PII, and whether it breached this duty;

d. Whether Pingora breached its duties to Plaintiffs and the Class as a result of the Data Breach;

e. Whether Pingora failed to provide adequate cyber security;

f. Whether Pingora knew or should have known that its computer and network security systems were vulnerable to cyber attacks;

g. Whether Pingora's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its company network;

h. Whether Pingora was negligent in permitting unencrypted PII off vast numbers of individuals to be stored within its network;

i. Whether Pingora was negligent in failing to adhere to reasonable retention policies, thereby greatly increasing the size of the Data Breach to include former employees and business associates;

j. Whether Pingora breached implied contractual duties to Plaintiffs and the Class to use reasonable care in protecting their PII;

k. Whether Pingora failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiffs and the Class;

l. Whether Pingora continues to breach duties to Plaintiffs and the Class;

m. Whether Plaintiffs and the Class suffered injury as a proximate result of Pingora's negligent actions or failures to act;

n. Whether Plaintiffs and the Class are entitled to recover damages, equitable relief, and other relief; and

o. Whether Pingora's actions alleged herein constitute gross negligence, and whether Plaintiffs and Class Members are entitled to punitive damages.

VII. CAUSES OF ACTION

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiffs and the Class)

90. Plaintiffs incorporate by reference all preceding factual allegations as though fully alleged here.

91. Defendant Pingora solicited, gathered, and stored the PII of Plaintiffs and the Class.

92. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and Class Members could and would suffer if the PII were wrongfully disclosed. Defendant had a duty to Plaintiffs and each Class Member to exercise reasonable care in holding, safeguarding, and protecting that information. Plaintiffs and the Class Members were the foreseeable victims of any inadequate safety and security practices. Plaintiffs and the Class Members had no ability to protect their PII that was in Pingora's possession. As such, a special relationship existed between Pingora and Plaintiffs and the Class.

93. Defendant was well aware of the fact that cyber criminals routinely target corporations through cyberattacks in an attempt to steal the PII of employees, applicants, business associates, and customers.

94. Defendant owed Plaintiffs and the Class Members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiffs and the Class when obtaining, storing, using, and managing personal information, including taking action to reasonably safeguard such data and providing notification to Plaintiffs and the Class Members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

95. Defendant's duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B.

96. Defendant had duties to protect and safeguard the PII of Plaintiffs and the Class from being vulnerable to cyberattacks, including by encrypting any document or report containing PII, by not permitting documents containing unencrypted PII to be maintained on its systems, and

other similarly common-sense precautions when dealing with sensitive PII. Additional duties that Pingora owed Plaintiffs and the Class include:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PII in its possession;
b. To protect the PII in its possession using reasonable and adequate security procedures and systems;
c. To adequately and properly audit and test its systems;
d. To adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store PII;
e. To train its employees not to store PII for longer than absolutely necessary;
f. To implement processes to quickly detect a data breach, security incident, or intrusion; and
g. To promptly notify Plaintiffs and Class Members of any data breach, security incident, or intrusion that affected or may have affected their PII.

97. Plaintiffs and the Class were the intended beneficiaries of Defendant's duties, creating a special relationship between them and Pingora. Defendant was in a position to ensure that its systems were sufficient to protect the PII that Plaintiffs and the Class had entrusted to it.

98. Defendant breached its duties of care by failing to adequately protect Plaintiffs' and Class Members' PII. Defendant breached its duties by, among other things:

a. Failing to exercise reasonable care in obtaining, retaining securing, safeguarding, deleting, and protecting the PII in its possession;
b. Failing to protect the PII in its possession using reasonable and adequate security procedures and systems;
c. Failing to adequately and properly audit and test its computer systems to avoid cyberattacks;

d. Failing to adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store PII, including maintaining PII in an encrypted format;

e. Failing to adequately and properly train its employees not to store PII for longer than absolutely necessary;

f. Failing to consistently enforce security policies aimed at protecting Plaintiffs and the Class's PII;

g. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions;

h. Failing to abide by reasonable retention and destruction policies for PII of former employees, applicants, business associates, and customers; and

i. Failing to promptly and accurately notify Plaintiffs and Class Members of the Data Breach that affected their PII.

99. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

100. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiffs and the Class have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

101. The damages Plaintiffs and the Class have suffered (as alleged above) were and are reasonably foreseeable.

102. The damages Plaintiffs and the Class have and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

103. Plaintiffs and the Class have suffered injury, including as described in Section IV.C, *supra*, and are entitled to actual and punitive damages in an amount to be proven at trial.

SECOND CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Class)

104. Plaintiffs incorporate by reference all preceding factual allegations as though fully alleged here.

105. Plaintiffs' and Class Members' PII was provided to Defendant as a condition of their mortgage loans.

106. When Plaintiffs and Class Members provided their PII to Defendant as part of their mortgage loan servicing, they entered into implied contracts in which Defendant agreed to comply with its statutory and common law duties to protect their PII and to timely notify them in the event of a Data Breach.

107. Based on Defendant's legal obligations and acceptance of Plaintiffs' and the Class Members' PII, Defendant had an implied duty to safeguard their PII through the use of reasonable industry standards.

108. Defendant breached the implied contracts by failing to safeguard Plaintiffs' and Class Members' PII and failing to provide them with timely and accurate notice of the Data Breach. Indeed, it took Pingora approximately four months to warn Plaintiffs and Class Member of their imminent risk of identity theft. Defendant also failed to notify Plaintiffs and the Class Members precisely what personal information was compromised, leaving Plaintiffs and Class Members unsure as to the extent of the information that was exposed.

109. As a direct and proximate result of Defendant's breach of implied contract, Plaintiffs and the Class Members have suffered damages, including foreseeable consequential damages that Defendant knew about when it requested Plaintiffs' and the Class Members' PII.

110. Plaintiffs and the Class have suffered injury, including as described in Section IV.C, *supra*, and are entitled to actual and punitive damages, statutory damages, and reasonable attorneys' fees and costs, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Class)

111. Plaintiffs incorporate by reference all preceding factual allegations as though fully alleged here.

112. Plaintiffs allege this claim in the alternative to its breach of implied contract claim.

113. Plaintiffs, and other Class Members, conferred a monetary benefit on Defendant by providing Defendant with profits from the servicing of Plaintiffs' and Class Members' mortgage loans.

114. Defendant appreciated that a monetary benefit was being conferred upon it by Plaintiffs and Class Members and accepted that monetary benefit.

115. However, acceptance of the benefit under the facts and circumstances outlined above make it inequitable for Defendant to retain that benefit without payment of the value thereof. Specifically, Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite data security.

116. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary benefit belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures.

117. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

118. If Plaintiffs and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

119. Plaintiffs and Class Members have no adequate remedy at law. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered or will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

120. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

121. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, all gains that they unjustly received.

FOURTH CAUSE OF ACTION
NEGLIGENCE *PER SE*
(On Behalf of all Plaintiffs and the Class)

122. Plaintiffs incorporate by reference all preceding factual allegations as though fully alleged here.

123. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII.

124. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders also form part of the basis of Defendant's duty in this regard.

125. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect consumers PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of a data breach including, specifically, the damages that would result to Plaintiffs and Class Members.

126. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se* as Defendant's violation of the FTC Act establishes the duty and breach elements of negligence.

127. Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

128. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses,

which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

129. In addition, Defendant's conduct violated Colo. Rev. Stat. § 6-1-713.5. Colo. Rev. Stat. § 6-1-713.5 requires commercial entities who maintain, own, or license "personal identifying information of an individual residing in the state" to "implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal identifying information and the nature and size of the business and its operations."

130. Defendant failed to comply with Colo. Rev. Stat. § 6-1-713.5. Specifically, Defendant voluntarily undertook the act of maintaining and storing Plaintiffs' PII, but Defendant failed to implement safety and security procedures and practices sufficient to protect from the data breach that it should have anticipated. Defendant should have known and anticipated that data breaches—especially breaches involving valuable information like mortgage loan data—were on the rise, and that mortgage banking institutions were lucrative or likely targets of cybercriminals looking to steal PII. As such, Defendant should have implemented and maintained procedures and practices appropriate to the nature and scope of information compromised in the data breach.

131. Plaintiffs and Class Members are within the class of persons that Colo. Rev. Stat. § 6-1-713.5 was intended to protect.

132. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

133. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

134. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known

that they were failing to meet their duties, and that Defendant's breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their PII.

135. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

FIFTH CAUSE OF ACTION
INJUNCTIVE AND DECLARATORY RELIEF
(On Behalf of all Plaintiffs and the Class)

136. Plaintiffs incorporate by reference all preceding factual allegations as though fully alleged here.

137. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

138. As previously alleged and pleaded, Defendant owes duties of care to Plaintiffs and Class Members that requires it to adequately secure their PII.

139. Defendant still possesses the PII of Plaintiffs and the Class Members.

140. Defendant has not satisfied its contractual obligations and legal duties to Plaintiffs and the Class Members.

141. Defendant has claimed that it is taking some steps to increase its data security, but there is nothing to prevent Defendant from reversing these changes once it has weathered the increased public attention resulting from this Breach, and to once again place profits above protection.

142. Plaintiffs, therefore, seek a declaration (1) that Defendant's existing security measures do not comply with its contractual obligations and duties of care to provide adequate security, and (2) that to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering Defendant to engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering Defendant to significantly increase its spending on cybersecurity including systems and personnel;

c. Ordering Defendant to engage third-party security auditors and internal personnel to run automated security monitoring;

d. Ordering that Defendant audit, test, and train their security personnel regarding any new or modified procedures;

e. Ordering that Defendant's segment Plaintiffs' and the Class's PII by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

f. Ordering that Defendant cease storing unencrypted PII on its systems;

g. Ordering that Defendant conduct regular database scanning and securing checks;

h. Ordering Defendant to routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

i. Ordering Defendant to implement and enforce adequate retention policies for PII, including destroying, in a reasonably secure manner, PII once it is no longer necessary for it to be retained; and

j. Ordering Defendant to meaningfully educate its current, former, and prospective employees and subcontractors about the threats they face as a result

of the loss of their financial and personal information to third parties, as well as the steps they must take to protect themselves.

VIII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs and the Class pray for judgment against Defendant as follows:

a. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Class requested herein;

b. A judgment in favor of Plaintiffs and the Class awarding them appropriate monetary relief, including compensatory damages, punitive damages, attorney fees, expenses, costs, and such other and further relief as is just and proper;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order requiring Defendant to pay the costs involved in notifying the Class Members about the judgment and administering the claims process;

e. A judgment in favor of Plaintiffs and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and

f. An award of such other and further relief as this Court may deem just and proper.

IX. DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury on all appropriate issues raised in this Class Action Complaint.

Dated: May 5, 2022

Respectfully submitted,

/s/ William B. Federman
William B. Federman
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
Telephone: (405) 235-1560
wbf@federmanlaw.com

A. Brooke Murphy
(*pro hac vice* forthcoming)
MURPHY LAW FIRM
4116 Will Rogers Pkwy, Suite 700
Oklahoma City, OK 73108
Telephone: (405) 389-4989
abm@murphylegalfirm.com

Attorneys for Plaintiffs